



PCT
533 Rec'd PCT/PTO 20 AUG 2001

501.40397X00

#5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): M. NISHIOKA, et al

Serial No.: 09/890,286

Filed: July 27, 2001

For: PUBLIC-KEY ENCRYPTION AND KEY-SHARING METHODS

Group: Not yet assigned

Examiner: Not yet assigned

RECEIVED

JAN 08 2002

Group 2100

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §1.97 & 1.98

Assistant Commissioner
for Patents
Washington, D.C. 20231

August 20, 2001

Sir:

In the matter of the above-identified application, applicants are submitting herewith copies of the documents listed in the attached form equivalent to Form PTO-1449 for the Examiner's consideration.

This information disclosure statement is being submitted within three months of the filing date.

Each of the documents listed on the attached form equivalent to Form PTO-1449 is in the English language.

It is respectfully requested that this information disclosure statement be considered by the Examiner.

Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to the deposit account of Antonelli, Terry, Stout & Kraus Deposit Account No. 01-2135

(501.40397X00) please credit any excess fees to such deposit account.

Respectfully submitted,



CIB/jdc
(703) 312-6600

Carl I. Brundidge
Registration No. 29,621
ANTONELLI, TERRY, STOUT & KRAUS, LLP



SHEET 1 OF 1

RECEIVED #5
JAN 08 2002
Group 2100FORM PTO-1449 U.S. Department of Commerce
(Rev. 4/92) Patent and Trademark OfficeINFORMATION DISCLOSURE
STATEMENT BY APPLICANT

(Use several sheets if necessary)

ATTY. DOCKET NO.

501.40397X00

SERIAL NO.

09/890,286

APPLICANT

M. NISHIOKA, et al

FILING DATE

July 27, 2001

GROUP

Not yet assigned

U.S. PATENT DOCUMENTS

DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLAS S	FILING DATE IF APPROPRIATE
DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLAS S	ABSTRACT
					YES NO
V. Miller, "Use of Elliptic Curves in Cryptography", <i>Exploratory Computer Science, IBM Research</i> , 1998, Springer-Verlag, pp. 417-426.					
R. Cramer, "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack", <i>Institute for Theoretical Computer Science, ETH Zurich</i> , 5/1998, pp. 1-18.					
M. Bellare, et al "Optimal Asymmetric Encryption", <i>Advance Networking Laboratory, IBM</i> , 1998 pp. 92-111.					
M. Bellare, et al "Relations Among Notions of Security for Public-key Encryption Schemes", 2/1999, <i>Advances in Cryptology, Crypto 98, Proceedings, Lecture Notes in Computer Science vol 1462</i> , pp. 1-30.					
M. Blum, "An Efficient Probabilistic Public-key Encryption Scheme which Hides All Partial Information", <i>Computer Science Department</i> , 1998, pp. 289-299.					
DATE CONSIDERED					

(Form PTO-1449 [6-4])